

REMARKS

In the Office Action mailed December 5, 2008, the Office noted that claims 16-18 were pending and rejected claims 16-18. Claims 16-18 have been amended, no claims have been canceled, claims 19-24 are new, and, thus, in view of the foregoing, claims 16-24 remain pending for reconsideration which is requested. No new matter has been added. The Office's rejections are traversed below.

REJECTIONS under 35 U.S.C. § 103

Claims 16-18 stand rejected under 35 U.S.C. § 103(a) as being obvious over Willenegger, U.S. Patent Publication No. 2003/0207696 in view of Sarkkinen, U.S. Patent Publication No. 2005/0015583. The Applicant respectfully disagrees and traverses the rejection with an argument and amendment.

Willenegger discusses a method for processing data for transmission to a plurality of terminals.

Sarkkinen discusses transmitting a message to a plurality of user entities in a network by using a multicast service, comprising the steps of encrypting a multicast message by using ciphering, and sending the encrypted multicast message to the plurality of user entities simultaneously.

On page 3 of the Office Action, it is acknowledged that Willenegger does not disclose "wherein the base station has a ciphering function of **preventing control signals and user**

information directed to the mobile station from being intercepted illegally in a radio section," as in claim 16. (Emphasis added) But instead, it is asserted that Sarkkinen ¶¶ 0108; 0112; and 0113 does.

However, nothing in Sarkkinen states that control signals are subject to the ciphering function. For example, Sarkkinen, Figs. 2 and 3 only show plain text blocks being encrypted and decrypted. Further, only ¶ 0028 of Sarkkinen explicitly mentions control signals and therein states:

Ciphering key generation related input parameters may be sent to the user entity when the user entity registers with a service sending encrypted messages to a plurality of user entities. Alternatively, ciphering key generation related input parameters may be sent to the user entity when a transmission of encrypted messages to a plurality of user entities is activated. **Thus, ciphering key generation related input parameters can be sent to the user entity by using normal control signalling.** [Emphasis added]

However, Sarkkinen ¶ 0046 states:

The **counter value** may be delivered to the plurality of users **unencrypted together with encrypted data**. Thus, it is not necessary to provide additional signalling since the counter value is transmitted together with the user data, i.e., the encrypted data packets. That is, the **counter value is delivered in conjunction with the content stream (in plain text via PTM channel), thus enabling the receivers to decrypt the content.** [Emphasis added]

Further, Sarkkinen ¶ 0104 states:

A time limited ciphering key can be taken care of by including an expiring time in a subscriber register (e.g. HLR/RRC), which indicates when the UE needs a new ciphering key. Therefore, each time when UE/NW activates e.g. any PDP context/RRC Connection to the UE in question, the ciphering key indication shall be checked from the register and a **new ciphering related**

information should be sent e.g. by using CN level signalling, SMS, RRC level signalling in UTRAN or peer to peer signalling between protocol layers, which are taken care of the multicast services) if indication defines that the old one has expired. [Emphasis added]

Thus, nowhere in Sarkkinen is it discussed that the control signals are encrypted in the base station to prevent them from being intercepted when sent to the mobile station in the radio section. As a whole, it appears that the signals in Sarkkinen are sent in the clear or at least portions are unencrypted therefore allowing them to be illegally received in a radio section.

Further, the Applicant has amended claim 16 to recite "wherein the base station has a ciphering function of preventing control signals and user information directed to the mobile station from being intercepted illegally in a radio section **of a RLC-TM (Radio Link Control - Transparent Mode) by using a ciphering counter,** and wherein the ciphering function **constructs the ciphering counter by combining** an HFN (Hyper Frame Number) and an SFN (Cell System Frame Number counter)." (Emphasis added) Support for the amendment may be found, for example, in ¶¶ 0018 and 0037 of the printed publication version of the Specification. The Applicant submits that no new matter is believed to have been added by the amendment of the claim.

According to the cited ¶ 0113 of Sarkkinen, COUNT-C (i.e. "ciphering counter") for RLC-TM consists of a combination of UFN/CFN, and COUNT-C for other RLC modes consists of a

combination of HFN/SFN, In contrast, the ciphering counter for RLC-TM in each of claims 16-18 consists of a combination of HFN/SFN.

Claims 17 and 18 have been amended in a similar manner. For at least the reasons discussed above, Willenegger and Sarkkinen, taken separately or in combination, fail to render obvious the features of claims 16-18.

Withdrawal of the rejection is respectfully requested.

NEW CLAIMS

Claims 19-24 are new. Support for claims 19-24 may be found, for example, in ¶¶ 0018 and 0046-0048 of the printed publication version of the Specification. The Applicant submits that no new matter is believed to have been added by the addition of the claims. The prior art of record fails to disclose when constructing the ciphering counter, the ciphering function initializes the HFN on a basis of an initial value included in ciphering parameters issued by the mobile station and sets the initialized HFN in the ciphering counter; and including a step of increasing the initialized HFN with a period of the SFN.

SUMMARY

It is submitted that the claims satisfy the requirements of 35 U.S.C. § 103. It is also submitted that claims 16-24 continue to be allowable. It is further submitted

that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston, Jr./
James J. Livingston, Jr.
Reg. No. 55,394
209 Madison St, Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/lrs